SANS

Test Yourself! - Unix Knowledge Quiz

Students who wish to take any of the following SANS courses:

- Track 6 – Securing Unix
- Track 8 - System Forensics, Investigations, and Response

should note that these courses require pre-existing knowledge of basic concepts relating to Unix.

We encourage students who want to attend any of these courses listed above to test their understanding of the prerequisite material using the following quiz.

Read the following questions, note your answers, and then check your results against the answer sheet provided. While this quiz alone cannot completely measure a student's readiness, it should be used as a guide to estimate your preparedness and help you to get the most out of your SANS course.

Quiz (60 questions)

1. Which of the following commands is used to list all packages and files installed via RPM?
a) "rpm -qa"
b) "rpm -query"
c) "rpm -q"
d) "rpm -q all"
Answer:_____

2. Which of the following is NOT TRUE regarding patches?
a) Vendors send patch updates to the administrators of the appropriate systems.
b) Computer security is never "static".
c) Vulnerabilities usually have been widely publicized for months.
d) Large numbers of systems are running vulnerable software.
Answer:_____

3. What is the main difference between "rpm -U" and "rpm -F"?
a) "rpm -U" is used for upgrading, "rpm -F" is not.
b) "rpm -F" only installs the new RPM if there is an older version, "rpm -U" does not.
c) "rpm -U" is ideal for patch installation, "rpm -F" is not.
d) "rpm -F" does not remove old version, "rpm -U" does.
Answer:_____

4. Which of the following is NOT TRUE regarding pre-compiled software?
a) Easy to install or update
b) Easier for attackers to distribute binaries with malicious code
c) Should download from trustworthy site
d) Validating downloads is not needed
Answer:_____

5. What does RPM stand for?
a) RedHat Package Manager
b) Redhot Patch Manager
c) Redhot Package Manager
d) RedHat Patch Manager
Answer:_____

6. Which of the following is the BEST reason administrators should always verify the cryptographic checksums on files they download?
a) To verify installation of the right version of software
b) Make sure software has not been corrupted
c) Avoid getting the wrong package
d) Avoid installing unneeded software
Answer:_____

7. Which of the following is the best way to keep software secure?
a) Downloading full binary versions of the updated software
b) Applying patches to source code and recompiling binaries
c) Installing binary patches to new software
d) Using automatic update tools
Answer:_____

8. Why are some of the most critical systems the LEAST up-to-date?
a) Busy testing before updating
b) Multiple services to update
c) Fear of disrupting system function
d) Patches not released fast enough
Answer:_____

9. Which of the following commands should be used for kernel patches?
a) "rpm -F"
b) "rpm -e"
c) "rpm -U"
d) "rpm -i"
Answer:_____

10. Which of the following is TRUE regarding RedHat's RPM-based patch management?
a) Intended as a patch management tool
b) Not intended to manage operating system packages
c) Easy to figure out current system patch level
d) Intended as a software distribution scheme
Answer:_____

11. Which of the following describes the last column of the inetd.conf?
a) Network port to listen on
b) Full path the binary inetd should run
c) The command wait or nowait
d) Whether the service is TCP or UDP-based

Answer:_____

12. Which of the following is a potential security problem when using GUI logins under a Unix system?
a) They allow remote devices to request similar login services
b) They disable GUI logins on non-desktop systems
c) They remove software from machines
d) Default allows local systems to request login
Answer:_____

13. Which of the following is NOT an extra built-in feature of xinetd over inetd?
a) More logging options
b) IP address based access control
c) Firing off various network servers on request
d) Support for warning banners
Answer:_____

14. Which of the following is NOT TRUE regarding login services (such as rlogin, rsh, etc)?
a) Passwords and information sent in clear text
b) Sessions can be easily hijacked
c) Weak authentication
d) Admin has control over critical login files (such as .rhosts)
Answer:_____

15. Which of the following commands is NOT valid?
a) chkconfig --level 2345 sendmail off
b) chkconfig sendmail off
c) chkconfig --list sendmail
d) chkconfig --reset sendmail
Answer:_____

16. Which of the following is NOT considered a small service?
a) echo
b) chargen
c) finger
d) discard
Answer:_____

17. Which of the following run levels will halt the system (as opposed to reboot)?
a) 0
b) 1
c) 4
d) 6
Answer:_____

18. Which of the following BEST describes what the kernel does on startup?
a) Prepares the system startup process
b) Starts every other service on the system

c) Requests username and password
d) Initializes and manages the system's hardware resources
Answer:_____

19. Which of the following is an easy configuration for securing sendmail?
a) Turning on mail daemon
b) Configuring relays so outgoing e-mail goes to central server
c) Processing sendmail queue periodically via Postfix
d) Running sendmail binary from disk
Answer:_____

20. Which of the following is TRUE regarding TFTP?
a) Secure
b) Requires username and password
c) Allows diskless workstations to boot
d) No restrictions
Answer:_____

21. How do you restart syslogd from systems other than RedHat?
a) pkill -HUP syslogd
b) kill -HUP <pid>
c) kill -HUP syslogd
d) syslogd restart
Answer:_____

22. Which of the following is TRUE regarding RedHat's logrotate.d?
a) Can be overridden by logrotate.conf
b) Specifies commands to run during rotation
c) Contains configuration file entry for each file to be rotated
d) Specifies time when logrotate should run
Answer:_____

23. Which of the following message facilities was formerly used by older e-mail servers and is not used much anymore?
a) mail
b) user
c) auth
d) comm
Answer:_____

24. Which of the following is TRUE regarding warning banners?
a) Very little debate on the subject of banners
b) Banners should conform to universal policies and guidelines
c) One size fits all in terms of banner messages
d) Legal ramifications yet to be clearly defined for them
Answer:_____

25. Which of the following is a benefit of system accounting?
a) Collects extraneous data

b) Catches abnormal performance
c) Detects intruders due to changes in system software
d) Not useful for justifying new hardware
Answer:_____

26. Which of the following is NOT found in the syslog.conf file?
a) Facility
b) Priority
c) Where messages should be sent
d) File permissions
Answer:_____

27. Which of the following is NOT normally contained in a warning message?
a) System is for authorized uses only
b) Some form of contact information
c) System may be monitored
d) Data can be shared with law enforcement officials
Answer:_____

28. Other than re-reading its configuration file, which of the following BEST describes what syslogd will do when issuing it the HUP signal?
a) Create new log files if they do not exist
b) Close all associated processes
c) Close any log files to which it may be writing and re-open all files listed in /etc/syslog.conf
d) Queue messages until log files exist
Answer:_____

29. Which of the following message facilities is ONLY used on Linux and not on other Unix operating systems?
a) authpriv
b) auth
c) cron
d) user
Answer:_____

30. Which of the following is TRUE regarding warning banners?
a) Improve overall security
b) Help understand what has happened on a system
c) May be required in order to prosecute under local computer crime statutes
d) Active approach
Answer:_____

31. What is the largest UID possible on most Unix systems?
a) 65534
b) 65535
c) 65536
d) 4294967295
e) 4294967294

Answer:_____

32. What is the usual name of sudo's configuration file?
a) /var/sudoers
b) /etc/sudoers
c) /etc/sudo
d) /usr/local/etc/sudoers
e) /usr/bin/sudoers
Answer:_____

33. Under which UID range are default system accounts created in Linux?
a) 0 - 499
b) 0 - 1024
c) 0 - 99
d) 0 - 49
Answer:_____

34. In general, BIOS passwords are LEAST suitable for which types of machines?
a) Desktops
b) Servers
c) Laptops
d) Public kiosks
Answer:_____

35. Which of the following is NOT TRUE regarding NFS?
a) Uses local UID to determine file access
b) If unique UIDs aren't used, other users can get access to files they do not own
c) Uses username to determine access to files
d) NFS looks up the username in local /etc/passwd file
Answer:_____

36. Which of the following is NOT TRUE regarding UNIX usernames and passwords?
a) Usernames are case-sensitive
b) Control sequences can be used on some systems
c) Usernames are limited to 9 characters for backwards compatibility
d) Passwords are case-sensitive
Answer:_____

37. Which of the following is the least secure method of getting root access on a system?
a) Using su
b) Console login
c) Using sudo
d) Login over telnet
Answer:_____

38. Which of the following forms of encryption is NOT used for passwords in standard OS installations?
a) DES56
b) MD5

c) Blowfish
d) RSA
Answer:_____

39. Which of the following is NOT a way to block logins to an account?
a) Put in *LOCKED* in the password string in /etc/shadow
b) Remove the password string from /etc/shadow
c) Change the shell in /etc/passwd to /dev/null
d) Put in =np= in the password sting in /etc/shadow
Answer:_____

40. Which of the following is TRUE regarding the UID and superuser account?
a) Other superuser accounts are locked out
b) The superuser account named root will be the only one with superuser access
c) Only one account can have superuser privileges
d) The superuser account is UID 0
Answer:_____

41. What Unix mount options should be used with BOTH floppies and CD-ROMs?
a) nosuid and ro
b) nodev, nosuid, and ro
c) nosuid and ro
d) nosuid and nodev
Answer:_____

42. How might an attacker with local access force a system reboot?
a) Force a shutdown from CD-ROM
b) Unplug the machine's power cord
c) Replace the keyboard with one with a "reboot" button
d) Use the local terminal to gain root access
Answer:_____

43. How can a normal user override soft limits set in /etc/security/limits.conf?
a) The ulimit command
b) Change limits.conf
c) Cannot override soft limits
d) The softlim command
Answer:_____

44. What RedHat command lists all the kernel network parameters that can be modified and their current values?
a) sysctl -a
b) top -n
c) netuse -r
d) ps -i
Answer:_____

45. On a system with only one actual network interface, what additional interface must be taken into account?

a) The null interface
b) The anonymous interface
c) The loopback interface
d) The shadow interface
Answer:_____

46. What is the function of the following Unix command?<p>chmod g+w myfile<p>
a) Set user execute
b) Set group write
c) Set all read
d) Set other sticky
Answer:_____

47. To set the default permission flags for new files in a directory to "only owner has access," what Unix command would you use?
a) umask 733
b) umask 700
c) umask 033
d) umask 077
Answer:_____

48. What will the Unix chown command generally do when the owner of a file changes, to help preserve security?
a) Strip the sticky bit
b) Strip the set-UID and set-GID bits
c) Check a root-owned file for authorization
d) Change the file's permission settings to 600
Answer:_____

49. Where does RedHat store cron logs by default?
a) /etc/log
b) /usr/cron
c) /var/log/cron
d) /dev/log/cron
Answer:_____

50. On RedHat install, who is allowed to execute the reboot or halt commands from the command line to shutdown the machine?
a) Root only
b) Root and root designates
c) Any user
d) All users but guests
Answer:_____

51. What option can you use with the Unix "ls" command to display file attributes?
a) "-d"
b) "-a"
c) "-l"
d) "-x"

Answer:_____

52. What would the file permission example "rwsr-sr-x" translate to in absolute mode?
a) 6755
b) 1644
c) 1755
d) 6645
Answer:_____

53. You have been called out to your client's site to investigate a suspected security incident on their production ecommerce server. For now, this is classified as a "suspected incident," because no one is sure whether or not the machine was actually attacked. Your job is to find out whether the machine has been successfully attacked, without bringing the system down until you are sure. You have identified a set of files you'd like to take offline for further analysis. Which of the following tools should you use to copy these to tape?
a) dd
b) tar
c) dump
d) cp
Answer:_____

54. Which of the following options directs "tar" to extract files from an archive?
a) -e
b) -a
c) -c
d) -p
e) -x
f) -f
Answer:_____

55. Which of the following options to "tar" would you use to examine the contents of an archive without extracting it?
a) -c
b) -x
c) -f
d) -v
e) -p
f) -t
Answer:_____

56. Using GNU tar, what's the simplest way to create a compressed archive from the contents of the current directory?
a) tar cfp - . | gzip > /tmp/archive.tar.gz
b) tar cfp archive.tar . ; gzip archive.tar
c) tar cfpz /tmp/archive.tar.gz .
d) tar cfp /tmp/archive.tar.gz .
Answer:_____

57. Which of the following utilities captures inode information for the files and directories it archives?
a) tar
b) cpio
c) cp
d) dump
Answer:_____

58. You want to copy the entire hard drive of a linux machine to a tape. You've booted the system from a live CDROM distribution of Linux, so the hard drive is idle. Which "dd" command would you use to create the disk image?
a) dd -i /dev/hda -o /dev/nst0
b) dd -i /dev/nst0 -o /dev/nst1
c) dd if=/dev/hda of=/dev/nst0
d) dd if=/dev/nst0 of=/dev/nst1
e) dd if=/dev/nst0 of=/dev/hda
Answer:_____

59. You want to write an image of a local hard drive to tape, but you cannot attach a tape drive to the local host. You have a machine called elocker elsewhere on the network which already has a tape drive. Which of the following commands could you use to write to that tape over the network?
a) dd if=/dev/hda of=elocker:/dev/nrst0
b) dd if=/dev/hda | ssh elocker > /dev/nrst0
c) dd if=/dev/hda | ssh elocker dd of=/dev/nrst0
d) ssh elocker dd if=/dev/hda | dd of=/dev/nrst0
Answer:_____

60. You have created several tar archives and written them all to the same tape using "dd." While verifying your archives, you notice that the tape only contains the last archive you wrote. Barring an OS bug or a hardware problem of some sort, what is the most likely cause for this?
a) You did not use the "no-rewind" device when writing your archives
b) You forgot to use dd's "conv=swab" option when reading the tapes back in
c) You should have used "mt fsf 1" between each dump to advance to the next file on the tape.
d) The "dd" program didn't write an end-of-file mark to the tape after each dump, so they were all concatenated into one large file, which confused tar when you verified the tape.
Answer:_____